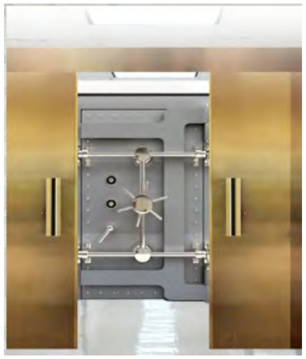
Copier and Office Equipment Security Risks

Peter Cybuck

Sharp Electronics

Sharp Imaging and Information Company of America



Quality Partnership Presentation

Threats and Mitigations
Federal Policies
Federal Laws

What you need to know about your office equipment in the era of cyber threats.

Acquisition of digital office equipment requires a clear appreciation the risks they bring and clear understanding of a new generation of office equipment specifications.

The greatest threat today in federal facilities comes from the insiders.
The individuals badged for the facility and authorized to use the office equipment

Multifunctional Product Vulnerabilities
What Are the Issues?

IEEE P2600

Standards workgroup focused on hardcopy security.

Nearly 200 Vulnerabilities Identified

Multifunctional Product Vulnerabilities

What Are the Issues?

Copier Use Is Anonymous

Copier E Mail Can Be Anonymous

Copier retains sensitive document data

Hard Drive - Flash
RAM

Copier may use a vulnerable PC Operating System exposing the office to viruses and other attacks

Admin Utilities Can Pose Risks - Loss of control - disclosed passwords

Unlike a PC there may be no user audit trail to track abuse

The copier software / firmware can be modified by attackers

Prints can be viewed by anyone

Copier can be a launch pad for
A network denial of service attack

Copier network Interface has PC like vulnerabilities

What is your liability? Is the copier Creating a risk of identify theft, of illegal disclosure of confidential information? Is it being used in violation of federal policies? Do buyers understand the security issues and risks?

Cybuck

A single feature or option won't cover the issues.

Multiple layers of security are required.

A suite of integrated complementary solutions provide the best defense.

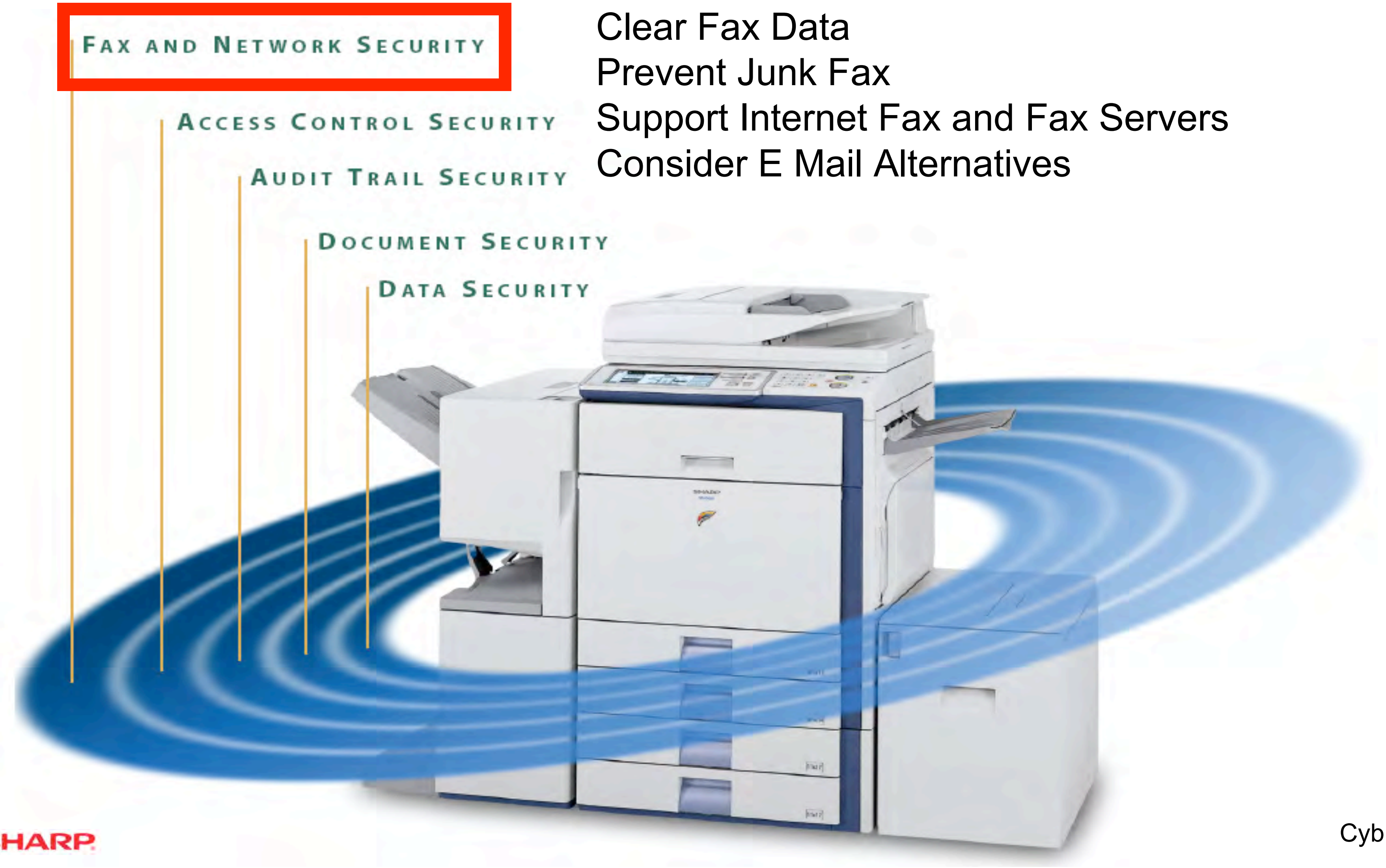
SHARP

Cybuck

Layered Security

FAX

Separation between Telephone network and LAN
Secure Fax Release
Clear Fax Data
Prevent Junk Fax
Support Internet Fax and Fax Servers
Consider E Mail Alternatives

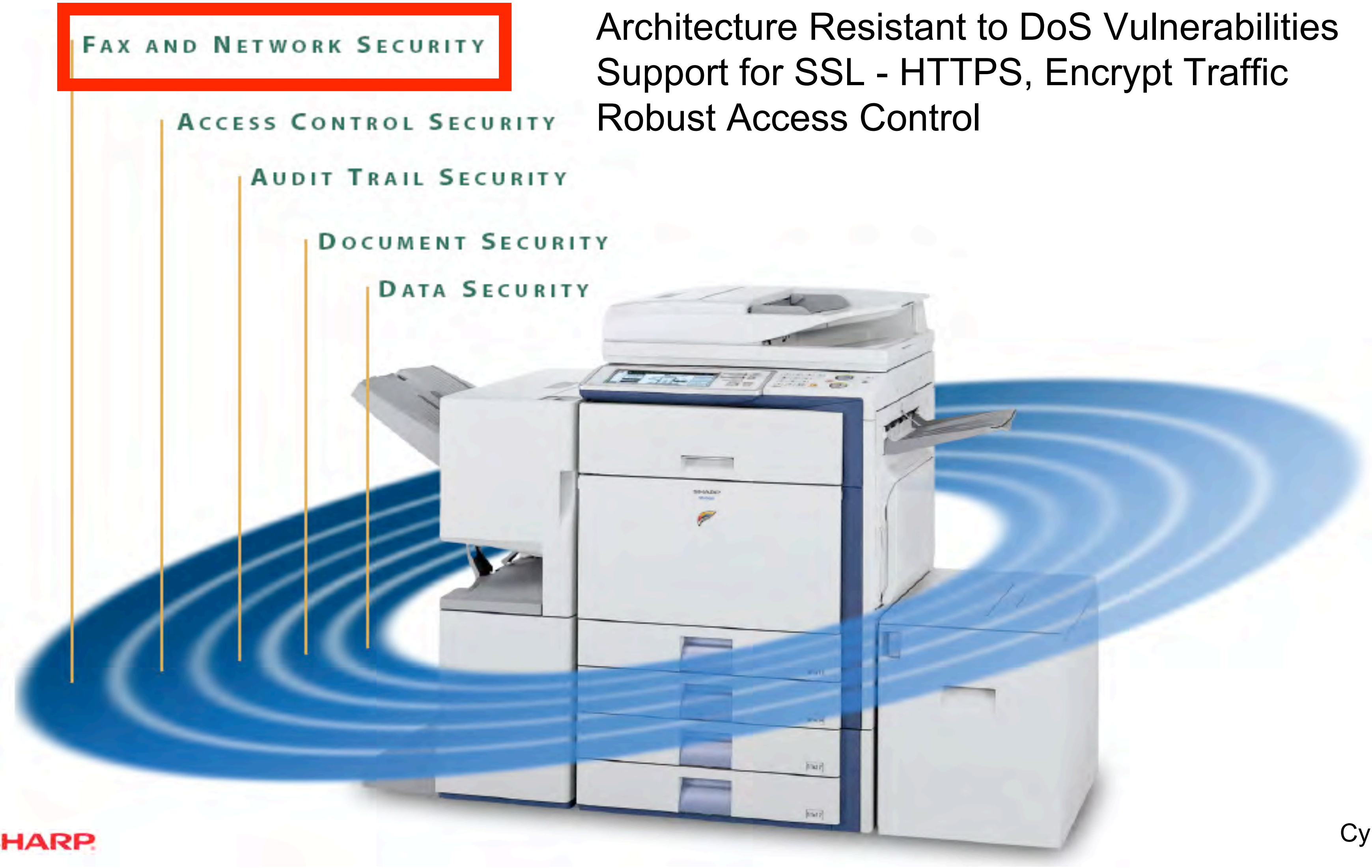


Fax and Network Security
Access Control Security
Audit Trail Security
Document Security
Data Security

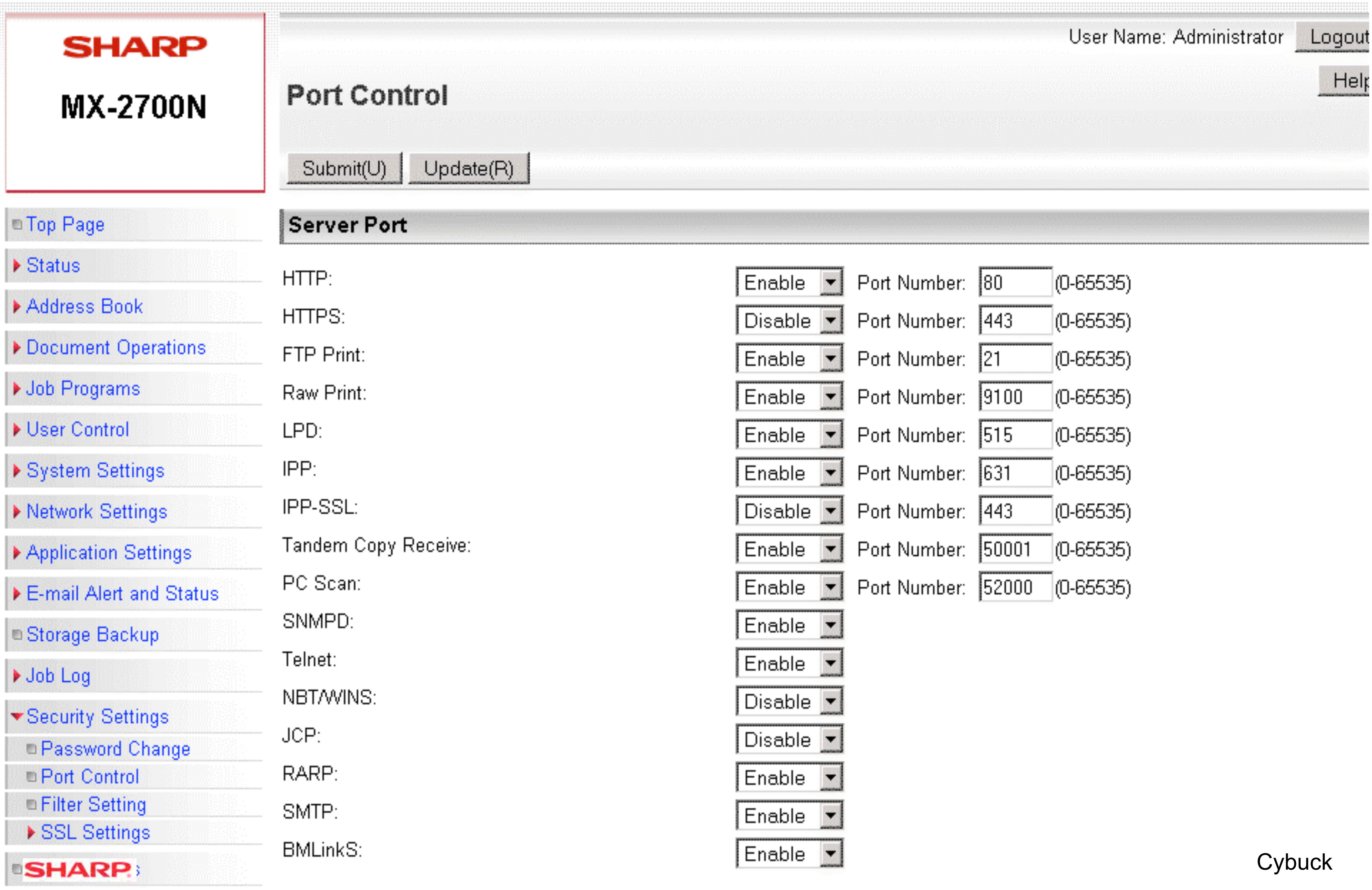
Layered Security

Network

Port Management and Filtering
Architecture Resistant to Viruses
Architecture Resistant to DoS Vulnerabilities
Support for SSL - HTTPS, Encrypt Traffic
Robust Access Control



Network Security - The copier today needs an integrated Firewall with complete administrator control over network ports.



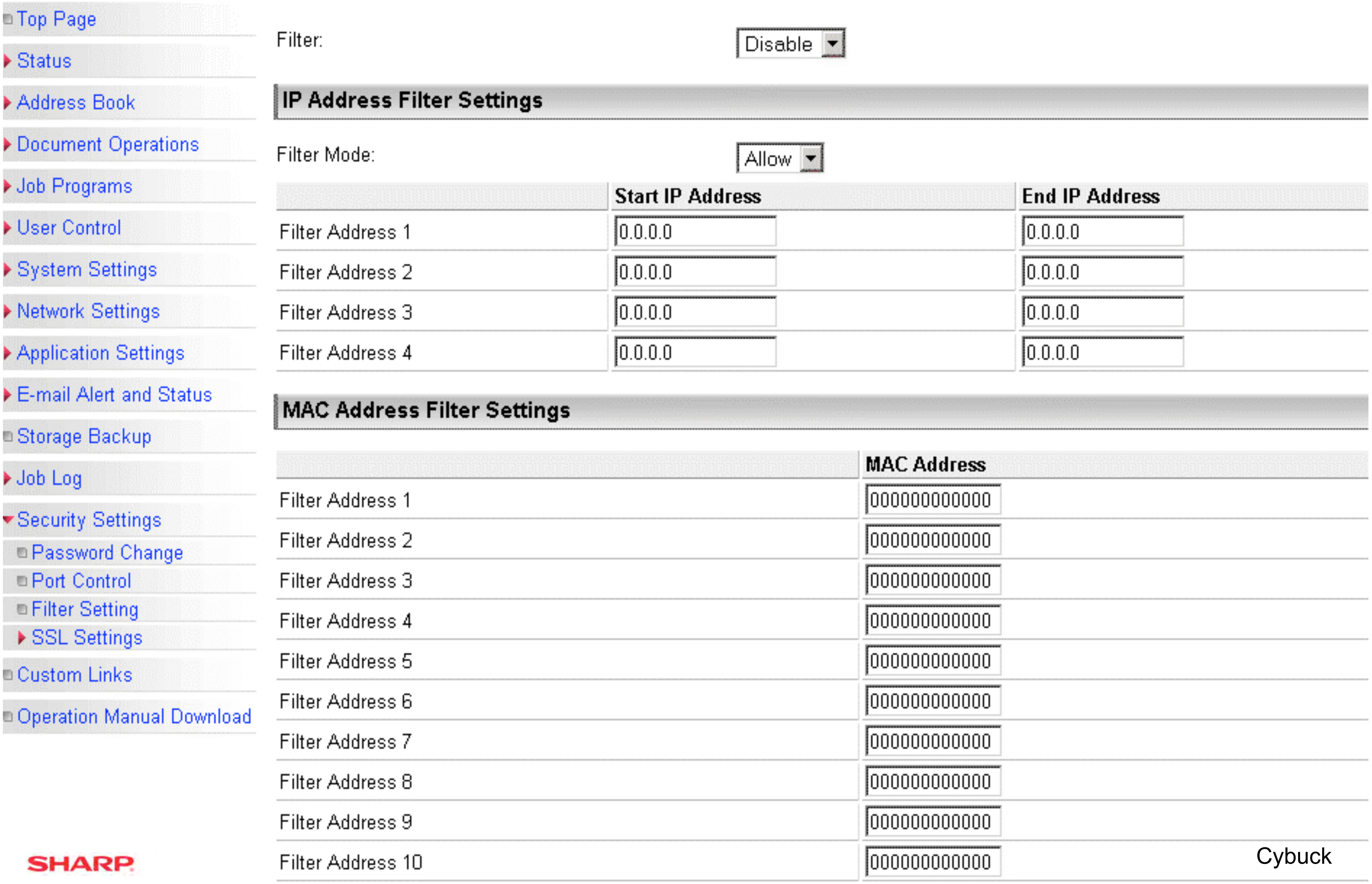
Port Control

Server Port

HTTP:	Enable	Port Number:	80	(0-65535)
HTTPS:	Disable	Port Number:	443	(0-65535)
FTP Print:	Enable	Port Number:	21	(0-65535)
Raw Print:	Enable	Port Number:	9100	(0-65535)
LPD:	Enable	Port Number:	515	(0-65535)
IPP:	Enable	Port Number:	631	(0-65535)
IPP-SSL:	Disable	Port Number:	443	(0-65535)
Tandem Copy Receive:	Enable	Port Number:	50001	(0-65535)
PC Scan:	Enable	Port Number:	52000	(0-65535)
SNMPD:	Enable			
Telnet:	Enable			
NBT/WINS:	Disable			
JCP:	Disable			
RARP:	Enable			
SMTP:	Enable			
BMLinkS:	Enable			

Cybuck

Network Security - Filtering out direct connections not approved prevents unauthorized use. Require IP and Mac address filtering.



Filter: Disable

IP Address Filter Settings

Filter Mode: Allow

	Start IP Address	End IP Address
Filter Address 1	0.0.0.0	0.0.0.0
Filter Address 2	0.0.0.0	0.0.0.0
Filter Address 3	0.0.0.0	0.0.0.0
Filter Address 4	0.0.0.0	0.0.0.0

MAC Address Filter Settings

	MAC Address
Filter Address 1	000000000000
Filter Address 2	000000000000
Filter Address 3	000000000000
Filter Address 4	000000000000
Filter Address 5	000000000000
Filter Address 6	000000000000
Filter Address 7	000000000000
Filter Address 8	000000000000
Filter Address 9	000000000000
Filter Address 10	000000000000

Cybuck

Layered Security

Threats and Mitigations

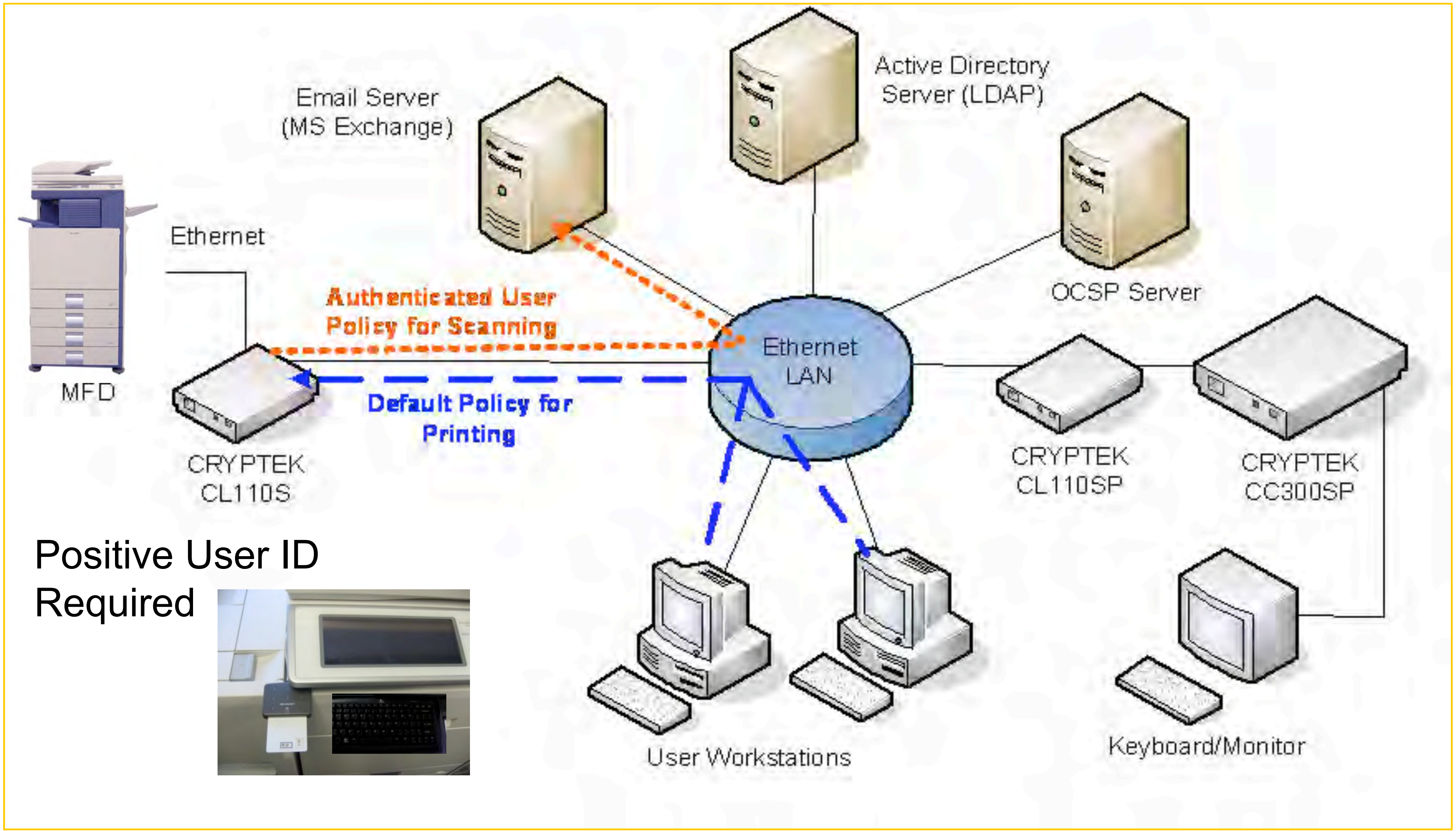
Access Control

Local User Authentication - Strong Passwords
Option of Smart Card control of access to network
Network Authentication - Active Directories
User Profiles control copy, print, file, scan, …
Full Qwerty keypad required

FAX AND NETWORK SECURITY
ACCESS CONTROL SECURITY
AUDIT TRAIL SECURITY
DOCUMENT SECURITY
DATA SECURITY
SHARP

Cybuck

Government Users will require Common Access Cards (CAC) to reach network services such as E Mail and Document Management Systems



Positive User ID Required

Unless your networked copier can be controlled by a CAC you might not be able to deploy scanning applications.

Cybuck

Layered Security

Threats and Mitigations

Audit Trail

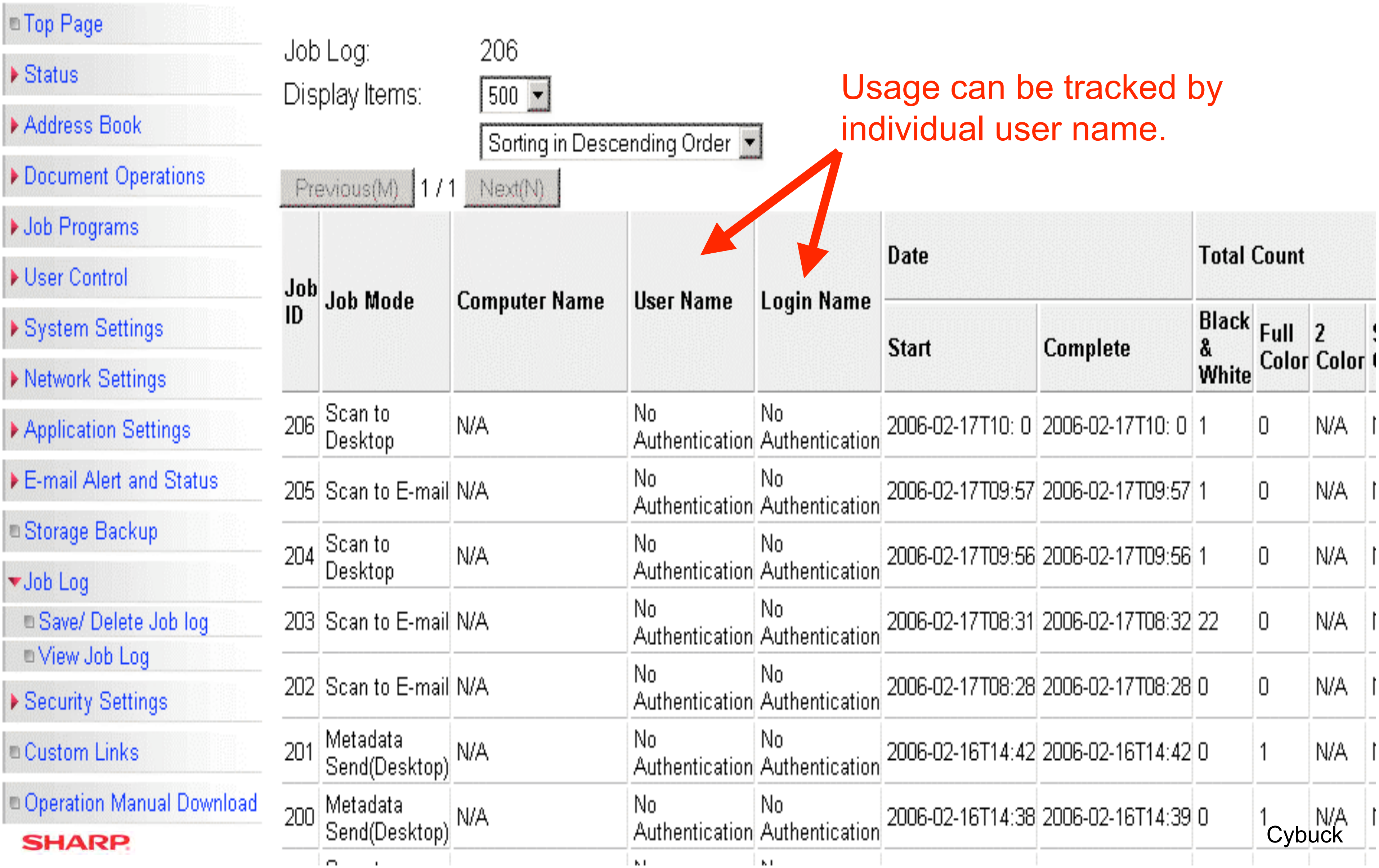
MFD Based log of all user activity including
Copy, print, scan, fax, E Mail
Options for network based robust audit records
Such as Equitrac Office - conventional and OSA based

FAX AND NETWORK SECURITY
ACCESS CONTROL SECURITY
AUDIT TRAIL SECURITY
DOCUMENT SECURITY
DATA SECURITY

SHARP

Cybuck

MFDs today can keep detailed usage records assuring compliance with new privacy laws and providing what is required to prove that compliance when audits are held.



Job Log: 206

Display Items: 500

Sorting in Descending Order

Job ID	Job Mode	Computer Name	User Name	Login Name	Date		Total Count		
					Start	Complete	Black & White	Full Color	2 Color
206	Scan to Desktop	N/A	No Authentication	No Authentication	2006-02-17T10: 0	2006-02-17T10: 0	1	0	N/A
205	Scan to E-mail	N/A	No Authentication	No Authentication	2006-02-17T09:57	2006-02-17T09:57	1	0	N/A
204	Scan to Desktop	N/A	No Authentication	No Authentication	2006-02-17T09:56	2006-02-17T09:56	1	0	N/A
203	Scan to E-mail	N/A	No Authentication	No Authentication	2006-02-17T08:31	2006-02-17T08:32	22	0	N/A
202	Scan to E-mail	N/A	No Authentication	No Authentication	2006-02-17T08:28	2006-02-17T08:28	0	0	N/A
201	Metadata Send(Desktop)	N/A	No Authentication	No Authentication	2006-02-16T14:42	2006-02-16T14:42	0	1	N/A
200	Metadata Send(Desktop)	N/A	No Authentication	No Authentication	2006-02-16T14:38	2006-02-16T14:39	0	1	N/A

Usage can be tracked by individual user name.

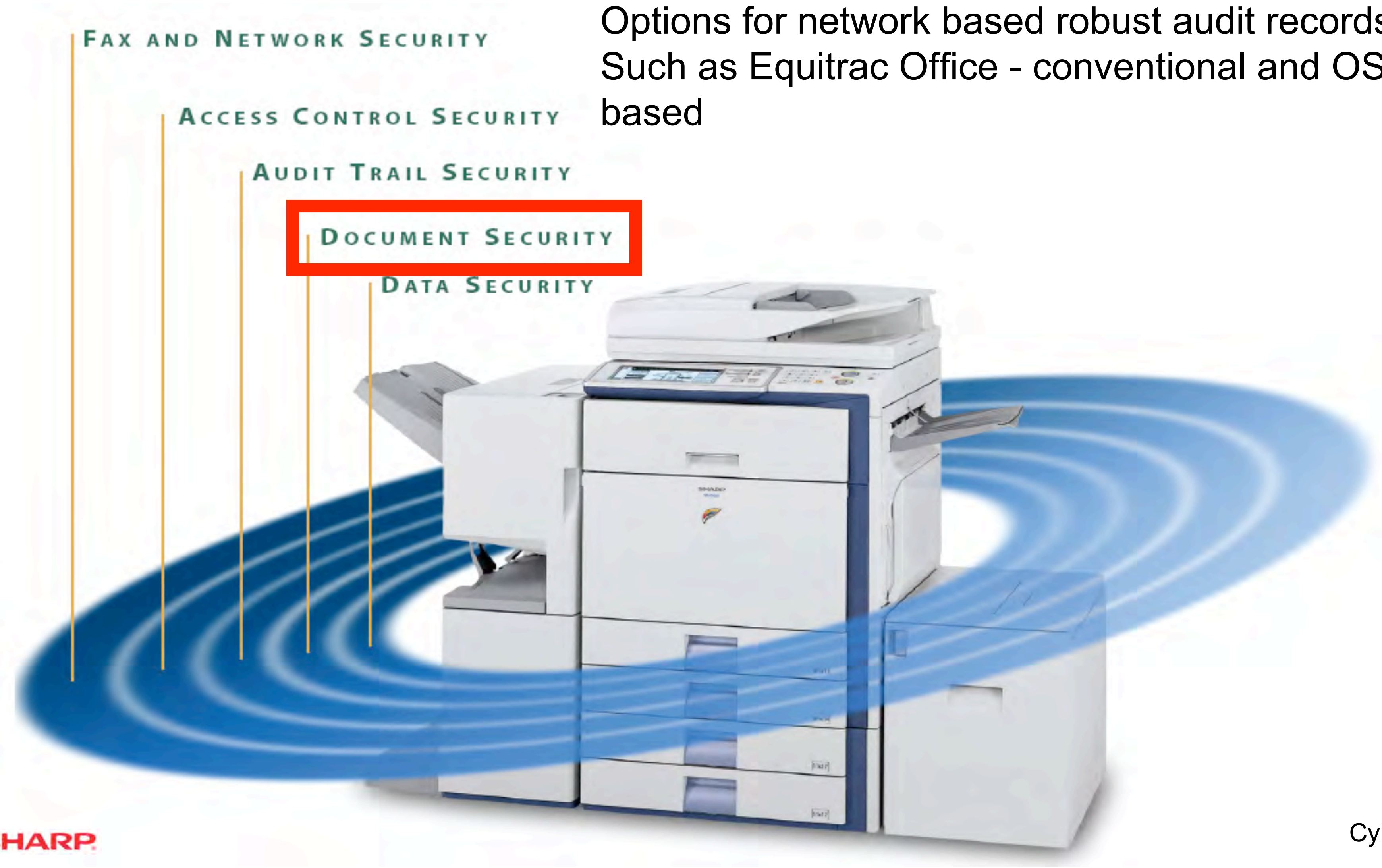
Cybuck

Layered Security

Threats and Mitigations

Document Security

MFD Based log of all user activity including
Copy, print, scan, fax, E Mail
Options for network based robust audit records
Such as Equitrac Office - conventional and OSA
based



SHARP

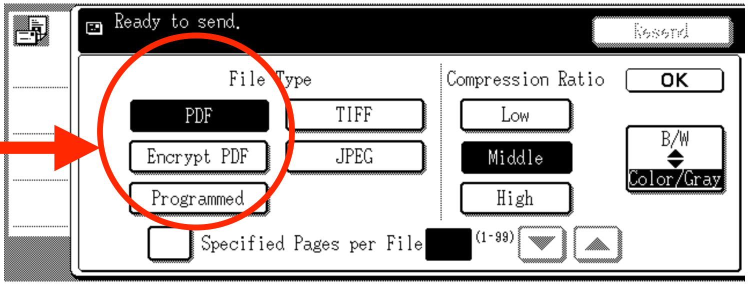
Cybuck

Secure Scanned Documents

The privacy of personal information such as personnel records, health records and financial records must be assured. Multi-functional copiers that can transmit information through public networks require new safeguards.

New Option

Select Encrypt PDF



Ready to send.

Option:
Scan to a secured local desktop and used IA approved communications software to transmit the originals captured by the copier scanner.

Recommendation:
Before you invest in dedicated network scanners consider using the copier’s networked scanner. It’s included at no additional charge.

Layered Security

Comprehensive Data Security

Secure automatic clearing of not only hard drives but RAM and Flash memory

Independent validation - Common Criteria

Use of encryption to assure protection in the event of power failures or hardware failures

Fax and Network Security
Access Control Security
Audit Trail Security
Document Security
Data Security

Data Security Kits for MFDs - Not all are alike!

❑ Multiple overwrites of data in magnetic memory (hard drives) up to seven times vs just clearing a directory or overwriting one to three times.

❑ Use of encryption to protect all buffered data so that if overwrites do not execute data is protected. Failure to execute usually requires service access.

❑ Use of encryption for print mailboxes and stored documents.

❑ Auto lockout after three failed password attempts for Admin, document file retrieval, encrypted PDFs …. Just like your computer.

❑ Document copy and scan control to disable reproduction of sensitive documents (print control pattern for color systems) … refuses to copy / scan

❑ Option to force Print and Fax hold operations - no prints in the open

❑ Restricted access to Address lists and configuration data - not just docs

❑ Certification - Common Criteria - At What EAL?- Does it work as advertised?

Multi-functional Copier Purchasing Decisions In the Networked Digital Office

The MFD decision has been shifting from facilities management staff, to Computer Information and Network management staff (IT), to Information Assurance - Security Staff (IA).

If IA does not approve the connection to the network, and the proposed applications, the acquired product may never be connected as a printer or a scanner.

If new policies regarding support for new protocols and controls (IPv6, SNMPv3, CAC, etc.) are not addressed by the MFD acquisition team the product may be obsolete one year into a five year contract.

The Multifunctional Copier is an IT device that must comply with federal policies addressing the processing of sensitive information. Security features play a major role in achieving compliance.

Multi-functional Device Purchase Criteria

The Classic Issues

Cost of Ownership
Contracts
Reliability
Features
Maintenance
Brand
Physical Size
Applications
Output Quality
Speed

Today’s New Issues

Security
Print and Copy Specific Security
Risk Management
Scan Specific Security and Authentication
Privacy Law Compliance
SCADA Related Threats
Common Criteria Certification (EAL)
Reports on NIST Vulnerability Database
IPv6, SNMPv3, Vista compatibility, …
Access Control - Common Access Card
Insider Abuse Controls and Audit Features
Network Security
Communications Security

Look for a new generation of
Security and IT Awards Presented To MFD Manufacturers.

SHARP

Cybuck

Copier and Office Equipment Security

QUESTIONS ???

Peter Cybuck

Sharp Electronics

Sharp Imaging and Information Company of America

Cybuckp@sharpsec.com

201-214-8760

Activity Monitoring and Logging
Robust, Flexible Control
Attack-Resistant OS
Powerful Memory and Hard Disk Protection
Extensive Firewall Protection
Advanced Encryption
Protection Against Fax Threats